Title (en)

METHOD FOR CRYPTOGRAPHIC SIGNING OF A DATA ITEM, ASSOCIATED ELECTRONIC DEVICE AND COMPUTER PROGRAM

Title (de)

VERFAHREN ZUR KRYPTOGRAPHISCHEN SIGNATUR EINER DATENINFORMATION, ELEKTRONISCHE VORRICHTUNG UND COMPUTERPROGRAMM DAFÜR

Title (fr)

PROCÉDÉ DE SIGNATURE CRYPTOGRAPHIQUE D'UNE DONNÉE, DISPOSITIF ÉLECTRONIQUE ET PROGRAMME D'ORDINATEUR ASSOCIÉS

Publication

EP 4239944 A1 20230906 (FR)

Application

EP 23150780 A 20230109

Priority

FR 2201866 A 20220303

Abstract (en)

[origin: CN116707814A] The invention relates to a method for cryptographically signing data, a related electronic device and a related computer program. A method for cryptographically signing data comprises:-(E10) determining a signature point equal to an element equal to a first derivation point plus a number equal to a first scalar,-(E12) determining a second scalar by subtracting a product of a third scalar and a fourth scalar from a product of the first scalar and a selected scalar,-(E14) determining another signature point,-(E14) determining a signature point equal to an element equal to the first derivation point plus a number equal to the first scalar,-(E14) determining a second scalar by subtracting a product of the third scalar and the fourth scalar from a product of the first scalar and the selected scalar. -(E16) determining the signature portion based on the private key, the first scalar, the coordinates of the signature points and the data,-(E16) determining the signature portion based on the private key, the first scalar, the coordinates of the signature points, and the data. The first derivation point and the second derivation point are equal to elements equal to the generation point plus numbers equal to the fifth scalar and the third scalar, respectively.

Abstract (fr)

Un procédé de signature cryptographique d'une donnée comprend les déterminations- (E10) d'un point de signature égal à l'addition d'éléments égaux à un premier point dérivé en nombre égal à un premier scalaire,- (E12) d'un deuxième scalaire en soustrayant au produit du premier scalaire et d'un scalaire sélectionné, le produit d'un troisième et d'un quatrième scalaires,- (E14) d'un autre point de signature égal à l'addition d'éléments égaux à un point sélectionné et en nombre égal au deuxième scalaire, et d'éléments égaux à un deuxième point dérivé et en nombre égal au quatrième scalaire.- (E16) d'une partie de signature à partir d'une clé privée, du premier scalaire, d'une coordonnée du point de signature et de la donnée,Le premier et le deuxième point dérivé sont respectivement égaux à l'addition d'éléments égaux à un point générateur en nombre égal à un cinquième et au troisième scalaires.

IPC 8 full level

H04L 9/00 (2022.01); **H04L 9/32** (2006.01)

CPC (source: CN EP KR US)

H04L 9/004 (2013.01 - EP); **H04L 9/0869** (2013.01 - US); **H04L 9/3066** (2013.01 - KR US); **H04L 9/3247** (2013.01 - KR US); **H04L 9/3249** (2013.01 - CN); **H04L 9/3252** (2013.01 - CN EP); H04L 2209/046 (2013.01 - KR); H04L 2209/08 (2013.01 - KR); H04L 2209/16 (2013.01 - EP); H04L 2209/72 (2013.01 - CN)

Citation (applicant)

S. CHOW ET AL.: "White Box Cryptography and an AES implementation", POST-PROCEEDINGS OF THE 9TH ANNUAL WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC'02, 15 August 2002 (2002-08-15)

Citation (search report)

- [A] EP 2553866 B1 20181121 - IRDETO BV [NL]
- [I] DOTTAX EMMANUELLE ET AL: "White-Box ECDSA: Challenges and Existing Solutions", 21 October 2021, ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, PAGE(S) 184 - 201, XP047614346

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

EP 4239944 A1 20230906; **EP 4239944 B1 20240320**; CN 116707814 A 20230905; FR 3133251 A1 20230908; FR 3133251 B1 20240322; JP 2023129381 A 20230914; KR 20230130540 A 20230912; US 2023283480 A1 20230907

DOCDB simple family (application)

EP 23150780 A 20230109; CN 202310099900 A 20230209; FR 2201866 A 20220303; JP 2023032322 A 20230302; KR 20230022302 A 20230220; US 202318168725 A 20230214